المركز الوطني للأمن السيبراني
National Cyber Security Center

بطاقة الوصف الوظيفي التحليلي

1. المعلومات الأساسية			
1.1 معلومات اساسية عن الوظيفة			
مسمى الوظيفــة	محلل أمن سيبراني مساعد	نوع الوظيفة	121
الدائرة	المركز الوطني للأمن السيبراني	الفئة الوظيفية	الأولى
الادارة/المديرية		المجموعة النوعية	
القسم/الشعبة		المستوى	الثالث
مسمى وظيفة الرئيس المباشر		المسمى القياسي الدال	محلل مساعد
رمز الوظيفة		مسمى الوظيفة الفعلي	محلل أمن سيبراني مساعد
حجم الموارد البشرية*		حجم موازنة الدائرة*	
*تعبأ لشاغلي وظائف المجموعة الثانية من الفئة العليا فقط.			

1.2 موقع الوظيفة في الهيكل التنظيمي للدائرة

تقع الوظيفة في إدارة العمليات والاستخبارات السيبرانية او إدارة الحوكمة السيبرانية وبناء القدرات الوطنية.

2. الغرض من الوظيفة

المهمة الرئيسية للوظيفة (الهدف من الوظيفة)

تختص الوظيفة بالارتقاء بالإدارة الاستباقية في التعامل مع التهديدات والثغرات السيبرانية وضمان الجاهزية الفورية لإدارة حوادث الامن السيبراني والاستجابة لها والتعامل مع الأضرار الناتجة عنها بهدف الاكتشاف المبكر لحوادث الامن السيبراني بناءً على عمليات المراقبة والتحليل واكتشاف الثغرات السيبرانية وإدارة التعامل معها والمساعدة في تنفيذ فحوصات الثغرات لتحديد الثغرات ونقاط الضعف الشائعة على المواقع الالكترونية والخوادم والتطبيقات والأنظمة وغيرها من الأصول الرقمية للوزارات والمؤسسات المختلفة للحماية من تعرضها لحوادث والتهديدات السيبرانية والحد منها ورفع مستوى الامان والحماية لها وفقا لقانون الامن السيبراني رقم 16 لسنة 2019.

3. المهام و الواجبات المسؤوليات الرئيسية

المهام التفصيلية والمسؤوليات

1. يساهم في المراقبة والتحليل الأولي للأحداث الأمنية.
2. يشارك في جمع وتحليل البيانات والسجلات الأمنية الأساسية.
3. يقدم الدعم لفريق الاستجابة للحوادث السيبرانية في تنفيذ الإجراءات الأولية وتوثيقها.
4. يساهم في أنشطة الاستخبارات السيبرانية وجمع وتحليل معلومات التهديدات.
5. يساعد في تطبيق السياسات والإجراءات الأمنية والمشاركة في عمليات التدقيق والامتثال..

المركز الوطني للأمن السيبراني
National Cyber Security Center

بطاقة الوصف الوظيفي التحليلي

6. يقوم بأية مهام أخرى يكلف بها ذات علاقة بطبيعة العمل.

4. مكونات الوظيفة

4.1 اتصالات العمل

ماهية وغرض الاتصال	جهات ومستوى الاتصال	مدى التكرار
○ تبادل معلومات روتينية متصلة بالعمل مباشرة. ○ تنسيق العمل. ○ توضيح أساليب العمل وطرقه أو تفسير البرامج والأعمال.	○ زملاء العمل المباشرين. ○ موظفين الوحدات الأخرى الوزارة/المؤسسة. ○ موظفي الدوائر الحكومية الأخرى.	○ يومياً.

4.2 المتطلبات الذهنية لحل مشكلات العمل.

قدرة متوسطة على التطبيق المباشر للمعرفة الأساسية بالعمل و تذكر بسيط لتتابع خطوات انجاز العمل، أو استيعاب حل المشاكل و الربط بين عناصر مختلفة والمسببات والنتائج و تحليل الظواهر أو المشاكل الى مكوناتها الأساسية أو تحليل المعلومات للتوصل الى نتائج و جمع أفكار متعددة لوضع فكرة جديدة أو التوصل الى الاستنتاجات من معطيات.

4.3 مجال العمل وتأثيره

أثر متوسط على أهداف التنظيم وعلاقته الداخلية والخارجية والأموال والممتلكات.

4.4 الصعوبة والتعقيد

أعمال متوسطة تتطلب إجراءات وأساليب وإجراءات وقواعد معرفة و ذات خطوات متعددة ومتداخلة ومتكرر.

4.5 المسؤولية الاشرافية

المسميات الوظيفية للمرؤوسين	درجة الوظيفة	أعداد الموظفين
-	-	-

4.6 المجهود البدني

(نوعية المجهود البدني (شدة المجهود البدني	النسبة المئوية من وقت العمل
جالس	100%

4.7 ظروف العمل

بيئة العمل	النسبة المئوية من وقت العمل
عادية (داخل المكتب)	100%

5. المؤهلات العلمية والخبرات العملية

5.1 متطلبات إشغال الوظيفة (الحد الأدنى من المؤهلات العلمية والخبرات العملية والتدريب)

5.1.1 المؤهل العلمي المطلوب (التعليم الأكاديمي، المهني، الخ)

المركز الوطني للأمن السيبراني
National Cyber Security Center

بطاقة الوصف الوظيفي التحليلي

البكالوريوس كحد أدنى في مجال الأمن السيبراني أو أمن الشبكات أو أمن المعلومات او علم الحاسوب أو هندسة وامن شبكات الحاسوب أو امن المعلومات والفضاء الالكتروني أي نخصص ذو علاقة

5.1.2 الخبرة العملية المطلوبة	
نوع الخبرة العملية ومجالها	مدة الخبرة العملية
بدون خبرة	———

5.1.3 التدريب الفني أو الإداري أو التخصصي المطلوب (ويقصد التدريب الرسمي اللازم لممارسة عمل او مهنة معينة قبل شغل الوظيفة)	
مستوى التدريب ومجاله	مدة التدريب
• اذا كان المؤهل العلمي (علم الحاسوب) يجب أن يكون حاصل على (3) دورات تدريبية التالية: 1. CompTIA Security+ 2. CompTIA Network+ 3. Certified Network Defender (CND) • يفضل أن يكون المتقدم حاصل على إحدى الدورات التدريبية التالية : 1. Certified Ethical Hacker (CEH) 2. ISO/IEC 27001 Lead Implementer 3. Lead Auditor 4. Cisco CCNA (Security Track)	-

5.2 الكفايات الوظيفية		
الكفاية المطلوبة	وصف الكفاية	مستويات اتقان الكفاية (اساسي، متوسط، متقدم، خبير(
الكفايات الفنية	تحليل الهجمات السيبرانية مراقبة البصمة والتواجد الرقمي مراقبة التحقق الأمني وفحص الاختراق استخبارات التهديدات والكشف عنها التحقيقات الجنائية السيبرانية حوكمة الامن السيبراني	إساسي إساسي إساسي إساسي إساسي اساسي
الكفايات القيادية (لشاغلي الوظائف الإشرافية والقيادية)	-	-
الكفايات العامة (السلوكية والإدارية)	احترافية الأداء التعاون والعمل بروح الفريق الالتزام بناء العلاقات الاتصال الفعال	اساسي اساسي إساسي اساسي اساسي